NATIONAL INSTITUTE OF TECHNOLOGY CALICUT

Department of Computer Science and Engineering

CS4062D: Introduction to Information Security (IIS)

Assignment-II

DATE of issue: 07-03-2022 **Date of submission: 20-03-2022, 11:59 PM**

Note: - Implement the following programs in NTL (Number Theory Library)

(For Number Theory library visit link https://libntl.org/)

1. Implement the RSA Public-key Cryptography by choosing all the preliminary parameters in **512** and **1024** bits.
2. Implement the El-Gamal Public-key Cryptography by choosing all the preliminary parameters in **512** and **1024** bits.
3. Implement the Elliptic Curve Cryptography (ECC) Public-key Cryptography over the prime field by choosing key size 163 bit NIST parameters.
4. Implement the digital signature using RSA, El-Gamal, and ECC with minimum key size.